

METHOD OF CIPHERING DATA TRANSMISSION IN A RADIO SYSTEM

Publication number: WO0054456 (A1)

Publication date: 2000-09-14

Inventor(s): VIALEN JUKKA [FI]; LONGONI FABIO [FI]

Applicant(s): NOKIA MOBILE PHONES LTD [FI]; VIALEN JUKKA [FI];
LONGONI FABIO [FI]

Classification:






- **international:** G09C1/00; H04L9/18; H04W12/02; G09C1/00; H04L9/18;
H04W12/00; (IPC1-7): H04L9/16

- **European:** H04W12/02; H04L9/18

Application number: WO2000FI00177 20000308



Priority number(s): FI19990000500 19990308

Also published as:

 US6882727 (B1)
 US2006120530 (A1)
 JP2002539490 (T)
 FI990500 (A)
 FI107487 (B1)

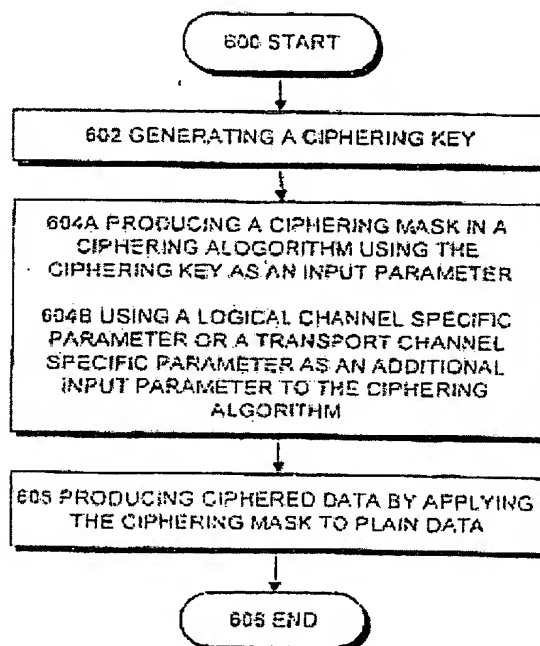
more >>

Cited documents:

 WO9712461 (A1)
 US5600722 (A)

Abstract of WO 0054456 (A1)

The invention relates to a method of ciphering data transmission in a radio system, and to a user equipment using the method, and to a radio network subsystem using the method. The method includes the steps of: (602) generating a ciphering key; (604A) producing a ciphering mask in a ciphering algorithm using the ciphering key as an input parameter; (604B) using a logical channel specific parameter or a transport channel specific parameter as an additional input parameter to the ciphering algorithm; and (606) producing ciphered data by applying the ciphering mask to plain data.



Data supplied from the *esp@cenet* database — Worldwide

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2002-539490

(P2002-539490A)

(43) 公表日 平成14年11月19日 (2002. 11. 19)

(51) Int.Cl. ⁷	識別記号	F I	テ-マコード* (参考)
G 0 9 C 1/00	3 1 0	G 0 9 C 1/00	3 1 0 5 J 1 0 4
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R 5 K 0 6 7

審査請求 未請求 予備審査請求 有 (全 48 頁)

(21) 出願番号 特願2000-604569 (P2000-604569)
 (86) (22) 出願日 平成12年3月8日 (2000. 3. 8)
 (85) 翻訳文提出日 平成13年9月7日 (2001. 9. 7)
 (86) 国際出願番号 P C T / F I 0 0 / 0 0 1 7 7
 (87) 国際公開番号 W O 0 0 / 5 4 4 5 6
 (87) 国際公開日 平成12年9月14日 (2000. 9. 14)
 (31) 優先権主張番号 9 9 0 5 0 0
 (32) 優先日 平成11年3月8日 (1999. 3. 8)
 (33) 優先権主張国 フィンランド (F I)

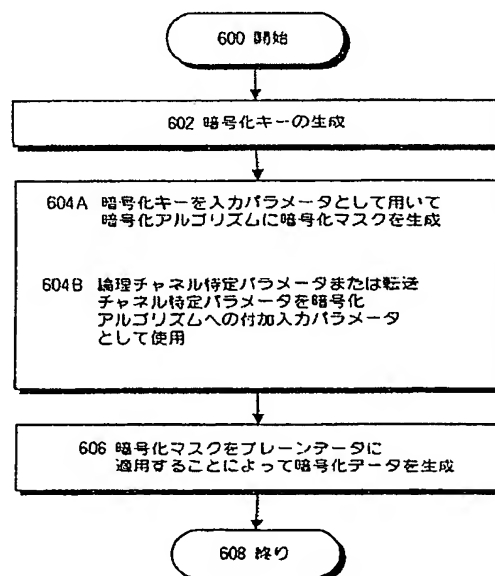
(71) 出願人 ノキア モービル フォーンズ リミティ
 ド
 フィンランド国, エフアイエヌ-02150
 エスポー, ケイララーデンティエ 4
 (72) 発明者 ビアレニ, ユッカ
 フィンランド国, エフイーエン-02320
 エスポー, ティルススキヤ 3 ベー 13
 (72) 発明者 ロンゴニ, ファビオ
 フィンランド国, エフイーエン-02130
 エスポー, ビサメキ 5 エー 38
 (74) 代理人 弁理士 石田 敬 (外4名)

最終頁に続く

(54) 【発明の名称】 無線システムのデータ伝送を暗号化する方法

(57) 【要約】

本発明は、無線システムのデータ伝送を暗号化する方法と、該方法を用いるユーザ装置と、該方法を用いる無線ネットワークサブシステムとに関する。前記方法は、
 (602) 暗号化キーを生成するステップと、(604A) 前記暗号化キーを入力パラメータとして用いて暗号化アルゴリズムに暗号化マスクを生成するステップと、
 (604B) 前記暗号化アルゴリズムへの付加入力パラメータとして論理チャネル特定パラメータまたは転送チャネル特定パラメータを用いるステップと、(606) 前記暗号化マスクをプレーンデータに適用することによって暗号化データを生成するステップと、を含む。



【特許請求の範囲】

【請求項1】 無線システムのデータ伝送を暗号化する方法であって、

(602) 暗号化キーを生成するステップと、

(604A) 前記暗号化キーを入力パラメータとして用いて暗号化アルゴリズムに暗号化マスクを生成するステップと、

(606) 前記暗号化マスクをプレーンデータに適用することによって暗号化データを生成するステップと、
を含む方法において、

(604B) 論理チャネル特定パラメータまたは転送チャネル特定パラメータを前記暗号化アルゴリズムへの付加入力パラメータとして用いることを特徴とする、無線システムのデータ伝送を暗号化する方法。

【請求項2】 前記暗号化アルゴリズムへの付加入力パラメータとして伝送方向を用いることを特徴とする請求項1に記載の方法。

【請求項3】 前記論理チャネル特定パラメータが、無線アクセスベアラ識別子、論理チャネル識別子、信号リンク識別子の1つであることを特徴とする請求項1に記載の方法。

【請求項4】 前記転送チャネル特定パラメータが専用チャネル識別子であることを特徴とする請求項1に記載の方法。

【請求項5】 前記暗号化アルゴリズムへの付加入力パラメータとして無線フレーム特定パラメータを用いることを特徴とする請求項1に記載の方法。

【請求項6】 前記無線フレーム特定パラメータがユーザ装置フレーム番号であることを特徴とする請求項5に記載の方法。

【請求項7】 前記プレーンデータが、少なくとも2つの並列論理チャネルからの無線リンク制御レイヤプロトコルデータユニットを含み、また各論理チャネルのために個々の暗号化マスクが生成されることを特徴とする請求項1に記載の方法。

【請求項8】 少なくとも1つの論理チャネルの無線リンク制御レイヤプロトコルデータユニットがすでに暗号化され、また暗号化データを生成する前記ステップが、前記すでに暗号化された無線リンク制御レイヤプロトコルデータユニ

ットのために繰り返されないことを特徴とする請求項7に記載の方法。

【請求項9】 前記プレーンデータが、1つの論理チャネルからの1つの無線リンク制御レイヤプロトコルデータユニットを含み、また前記論理チャネルのために個々の暗号化マスクが生成されることを特徴とする請求項1に記載の方法。

【請求項10】 前記プレーンデータが、1つの論理チャネルの少なくとも2つの連続した無線リンク制御レイヤプロトコルデータユニットを含み、また各無線リンク制御レイヤプロトコルデータユニットのために前記暗号化マスクの異なる部分が、前記暗号化データの生成に用いられることを特徴とする請求項1に記載の方法。

【請求項11】 前記プレーンデータが、少なくとも2つの異なる論理チャネルのメディアアクセス制御レイヤプロトコルデータユニットを含む1つの転送ブロックセットを含み、また各転送ブロックセットのために1つの暗号化マスクが、前記暗号化データの生成に用いられることを特徴とする請求項1に記載の方法。

【請求項12】 前記プレーンデータが、1つの論理チャネルのメディアアクセス制御レイヤプロトコルデータユニットを含む1つの転送ブロックセットを含み、また各転送ブロックセットのために1つの暗号化マスクが、前記暗号化データの生成に用いられることを特徴とする請求項1に記載の方法。

【請求項13】 前記暗号化が、プロトコルスタックのメディアアクセス制御レイヤで実施されることを特徴とする請求項1に記載の方法。

【請求項14】 新しい暗号化マスクが、前記プロトコルスタックの物理レイヤの各無線フレームのために生成されることを特徴とする請求項1に記載の方法。

【請求項15】 新しい暗号化マスクが、前記プロトコルスタックの物理レイヤの各インタリーブ期間のために生成されることを特徴とする請求項1に記載の方法。

【請求項16】 暗号化キー（410）を生成するための生成手段（408）と、

暗号化キー（４１０）を入力パラメータとして用いて暗号化マスク（４１２Ａ、４１２Ｂ、４１２Ｃ）を生成するための生成手段（４０８）と接続された暗号化アルゴリズム（４００）と、

暗号化マスク（４１２Ａ、４１２Ｂ、４１２Ｃ）をプレーンデータ（４１４Ａ、４１４Ｂ、４１４Ｃ）に適用することによって暗号化データ（４１８Ａ、４１８Ｂ、４１８Ｃ）を生成するための暗号化アルゴリズム（４００）と接続された暗号化手段（４１６Ａ、４１６Ｂ、４１６Ｃ）と、

を具備するユーザ装置（ＵＥ）において、

前記暗号化アルゴリズム（４００）が、論理チャネル特定パラメータ（４０２Ａ）または転送チャネル特定パラメータ（４０２Ｂ）を付加入力パラメータとして用いることを特徴とするユーザ装置。

【請求項１７】 前記暗号化アルゴリズム（４００）が、付加入力パラメータとして伝送方向を用いることを特徴とする請求項１６に記載のユーザ装置。

【請求項１８】 前記論理チャネル特定パラメータ（４０２Ａ）が、無線アクセスベアラ識別子、論理チャネル識別子、信号リンク識別子の１つであることを特徴とする請求項１６に記載のユーザ装置。

【請求項１９】 前記転送チャネル特定パラメータ（４０２Ｂ）が専用チャネル識別子であることを特徴とする請求項１６に記載のユーザ装置。

【請求項２０】 前記暗号化アルゴリズム（４００）が、無線フレーム特定パラメータ（４０４）を付加入力パラメータとして用いることを特徴とする請求項１６に記載のユーザ装置。

【請求項２１】 前記無線フレーム特定パラメータ（４０４）がユーザ装置フレーム番号であることを特徴とする請求項２０に記載のユーザ装置。

【請求項２２】 前記暗号化手段（４１６Ａ、４１６Ｂ、４１６Ｃ）が、少なくとも２つの並列論理チャネルからの無線リンク制御レイヤプロトコルデータユニットを含むプレーンデータ（４１４Ａ、４１４Ｂ、４１４Ｃ）を受け入れ、また暗号化アルゴリズム（４００）が、各論理チャネルのために個々の暗号化マスク（４１２Ａ、４１２Ｂ、４１２Ｃ）を生成し、暗号化手段（４１６Ａ、４１６Ｂ、４１６Ｃ）が、各論理チャネルのために前記チャネルの暗号化マスク（４

12A、412B、412C)を用いることを特徴とする請求項16に記載のユーザ装置。

【請求項23】 少なくとも1つの論理チャネルの無線リンク制御レイヤプロトコルデータユニット(414C)がすでに暗号化され、また暗号化手段(416C)が、前記すでに暗号化された無線リンク制御レイヤプロトコルデータユニット(414C)を暗号化しないことを特徴とする請求項22に記載のユーザ装置。

【請求項24】 前記暗号化手段(416A)が、1つの論理チャネルからの無線リンク制御レイヤプロトコルデータユニットを含むプレーンデータ(414A)を受け入れ、また暗号化アルゴリズム(400)が、前記論理チャネルのために個々の暗号化マスク(412A)を生成し、暗号化手段(416A)が、前記論理チャネルのために前記チャネルの暗号化マスク(412A)を用いることを特徴とする請求項16に記載のユーザ装置。

【請求項25】 前記暗号化手段(426)が、1つの論理チャネルの少なくとも2つの連続した無線リンク制御レイヤプロトコルデータユニットを含むプレーンデータを受け入れ、また暗号化アルゴリズム(400)が、前記論理チャネルのために個々の暗号化マスク(412A)を生成し、暗号化手段(426)が、各無線リンク制御レイヤプロトコルデータユニットのために暗号化マスク(412A)の異なる部分を用いることを特徴とする請求項16に記載のユーザ装置。

【請求項26】 前記暗号化手段(434)が、少なくとも2つの異なる論理チャネルのメディアアクセス制御レイヤプロトコルデータユニットを含む1つの転送ブロックセットを含むプレーンデータを受け入れ、また暗号化アルゴリズム(400)が、各転送ブロックセットのために個々の暗号化マスク(412)を生成し、暗号化手段(434)が、各転送ブロックセットのために1つの暗号化マスク(412)を用いることを特徴とする請求項16に記載のユーザ装置。

【請求項27】 前記暗号化手段(434)が、1つの論理チャネルのメディアアクセス制御レイヤプロトコルデータユニットを含む1つの転送ブロックセットを含むプレーンデータを受け入れ、また暗号化アルゴリズム(400)が、各

転送ブロックセットのために個々の暗号化マスク（412）を生成し、暗号化手段（434）が、各転送ブロックセットのために1つの暗号化マスク（412）を用いることを特徴とする請求項16に記載のユーザ装置。

【請求項28】 前記生成手段（408）、暗号化アルゴリズム（400）および暗号化手段（416A、416B、416C）が、プロトコルスタックのメディアアクセス制御レイヤに存在することを特徴とする請求項16に記載のユーザ装置。

【請求項29】 前記暗号化アルゴリズム（400）が、前記プロトコルスタックの物理レイヤの各無線フレームのための新しい暗号化マスク（412A、412B、412C）を生成することを特徴とする請求項16に記載のユーザ装置。

【請求項30】 前記暗号化アルゴリズム（400）が、前記プロトコルスタックの物理レイヤの各インタリーブ期間のための新しい暗号化マスク（412A、412B、412C）を生成することを特徴とする請求項16に記載のユーザ装置。

【請求項31】 暗号化キー（410）を生成するための生成手段（408）と、

暗号化キー（410）を入力パラメータとして用いて暗号化マスク（412A、412B、412C）を生成するための生成手段（408）と接続された暗号化アルゴリズム（400）と、

暗号化マスク（412A、412B、412C）をプレーンデータ（414A、414B、414C）に適用することによって暗号化データ（418A、418B、418C）を生成するための暗号化アルゴリズム（400）と接続された暗号化手段（416A、416B、416C）と、

を具備する無線ネットワークサブシステム（RNS）において、

前記暗号化アルゴリズム（400）が、論理チャネル特定パラメータ（402A）または転送チャネル特定パラメータ（402B）を付加入力パラメータとして用いることを特徴とする無線ネットワークサブシステム。

【請求項32】 前記暗号化アルゴリズム（400）が、伝送方向を付加入

力パラメータとして用いることを特徴とする請求項31に記載の無線ネットワークサブシステム。

【請求項33】 前記論理チャネル特定パラメータ(402A)が、無線アクセスベアラ識別子、論理チャネル識別子、信号リンク識別子の1つであることを特徴とする請求項31に記載の無線ネットワークサブシステム。

【請求項34】 前記転送チャネル特定パラメータ(402B)が専用チャネル識別子であることを特徴とする請求項31に記載の無線ネットワークサブシステム。

【請求項35】 前記暗号化アルゴリズム(400)が、無線フレーム特定パラメータ(404)を付加入力パラメータとして用いることを特徴とする請求項31に記載の無線ネットワークサブシステム。

【請求項36】 前記無線フレーム特定パラメータ(404)がユーザ装置フレーム番号であることを特徴とする請求項35に記載の無線ネットワークサブシステム。

【請求項37】 前記暗号化手段(416A、416B、416C)が、少なくとも2つの並列論理チャネルからの無線リンク制御レイヤプロトコルデータユニットを含むプレーンデータ(414A、414B、414C)を受け入れ、また暗号化アルゴリズム(400)が、各論理チャネルのために個々の暗号化マスク(412A、412B、412C)を生成し、暗号化手段(416A、416B、416C)が、各論理チャネルのために前記チャネルの暗号化マスク(412A、412B、412C)を用いることを特徴とする請求項31に記載の無線ネットワークサブシステム。

【請求項38】 少なくとも1つの論理チャネルの無線リンク制御レイヤプロトコルデータユニット(414C)がすでに暗号化され、また暗号化手段(416C)が、前記すでに暗号化された無線リンク制御レイヤプロトコルデータユニット(414C)を暗号化しないことを特徴とする請求項37に記載の無線ネットワークサブシステム。

【請求項39】 前記暗号化手段(416A)が、1つの論理チャネルからの無線リンク制御レイヤプロトコルデータユニットを含むプレーンデータ(41

4 A) を受け入れ、また暗号化アルゴリズム (4 0 0) が、前記論理チャネルのために個々の暗号化マスク (4 1 2 A) を生成し、暗号化手段 (4 1 6 A) が、前記論理チャネルのために前記チャネルの暗号化マスク (4 1 2 A) を用いることを特徴とする請求項 3 1 に記載の無線ネットワークサブシステム。

【請求項 4 0】 前記暗号化手段 (4 2 6) が、1つの論理チャネルの少なくとも2つの連続した無線リンク制御レイヤプロトコルデータユニットを含むプレーンデータを受け入れ、また暗号化アルゴリズム (4 0 0) が、前記論理チャネルのために個々の暗号化マスク (4 1 2 A) を生成し、暗号化手段 (4 2 6) が、各無線リンク制御レイヤプロトコルデータユニットのために暗号化マスク (4 1 2 A) の異なる部分を用いることを特徴とする請求項 3 1 に記載の無線ネットワークサブシステム。

【請求項 4 1】 前記暗号化手段 (4 3 4) が、少なくとも2つの異なる論理チャネルのメディアアクセス制御レイヤプロトコルデータユニットを含む1つの転送ブロックセットを含むプレーンデータを受け入れ、また暗号化アルゴリズム (4 0 0) が、各転送ブロックセットのために個々の暗号化マスク (4 1 2) を生成し、暗号化手段 (4 3 4) が、各転送ブロックセットのために1つの暗号化マスク (4 1 2) を用いることを特徴とする請求項 3 1 に記載の無線ネットワークサブシステム。

【請求項 4 2】 前記暗号化手段 (4 3 4) が、1つの論理チャネルのメディアアクセス制御レイヤプロトコルデータユニットを含む1つの転送ブロックセットを含むプレーンデータを受け入れ、また暗号化アルゴリズム (4 0 0) が、各転送ブロックセットのために個々の暗号化マスク (4 1 2) を生成し、暗号化手段 (4 3 4) が、各転送ブロックセットのために1つの暗号化マスク (4 1 2) を用いることを特徴とする請求項 3 1 に記載の無線ネットワークサブシステム。

【請求項 4 3】 前記生成手段 (4 0 8)、暗号化アルゴリズム (4 0 0) および暗号化手段 (4 1 6 A、4 1 6 B、4 1 6 C) が、プロトコルスタックのメディアアクセス制御レイヤに存在することを特徴とする請求項 3 1 に記載の無線ネットワークサブシステム。

【請求項44】 前記暗号化アルゴリズム（400）が、前記プロトコルスタックの物理レイヤの各無線フレームのための新しい暗号化マスク（412A、412B、412C）を生成することを特徴とする請求項31に記載の無線ネットワークサブシステム。

【請求項45】 前記暗号化アルゴリズム（400）が、前記プロトコルスタックの物理レイヤの各インタリーブ期間のための新しい暗号化マスク（412A、412B、412C）を生成することを特徴とする請求項31に記載の無線ネットワークサブシステム。

【発明の詳細な説明】**【0001】****発明の分野**

本発明は、無線システムのデータ伝送を暗号化する方法に関する。

【0002】**発明の背景**

今日、暗号化は、伝送されるデータが無資格のユーザの手に入るのを防止するために、多くのデータ伝送システムで用いられている。暗号化は、特に無線通信がより一般的になるに従い、過去数年において相当進歩している。

【0003】

暗号化は、例えば、送信機により伝送される情報を暗号化することによって、また受信機内の情報を解読することによって、行うことができる。暗号化手段では、伝送される情報、例えばビットストリームは、ある特定数の暗号化ビットパターンによって乗算され、この場合、使用した暗号化ビットパターンが未知であるならば、元のビットストリームが何であったかを見つけたことは困難である。

【0004】

例えば、デジタルGSMシステムでは、無線経路で暗号化が実行され、すなわち、無線経路に伝送すべき暗号化ビットストリームは、データビットと暗号化ビットとのXORをとることによって形成され、暗号化ビットは、暗号化キー K_c を用いて、それ自体公知のアルゴリズム（A5アルゴリズム）によって形成される。A5アルゴリズムは、トラフィックチャネルおよびDCH制御チャネルで伝送される情報を暗号化する。

【0005】

暗号化キー K_c は、ネットワークがターミナルを認証したが、チャネル上のトラフィックがまだ暗号化されていなかった場合に設定される。GSMシステムでは、ターミナルは、ターミナルに記憶されるインターナショナルモバイルサブスクライバアイデンティティ、IMSI、あるいは加入者識別子に基づき形成されるテンポラリモバイルサブスクライバアイデンティティ、TMSIに基づき識

別される。加入者識別キー K_i もターミナルに記憶される。ターミナル識別キーもシステムで認識される。

【0006】

暗号化の信頼性が高くなるように、暗号化キー K_c の情報は秘密に維持されなければならない。したがって、暗号化キーはネットワークからターミナルに間接的に伝送される。ランダムアクセス番号、 $RAND$ がネットワークに形成され、次に、その番号が基地局システムを介してターミナルに伝送される。暗号化キー K_c は、ランダムアクセス番号、 $RAND$ と加入者識別キー K_i とから公知のアルゴリズム（A5アルゴリズム）によって形成される。暗号化キー K_c は、ターミナルおよびシステムのネットワーク部分の両方において同一の方法で計算される。

【0007】

したがって、当初は、ターミナルと基地局との間の接続におけるデータ伝送は暗号化されない。基地局システムがターミナルに暗号化モード命令を送るまで、暗号化は開始しない。ターミナルが命令を受け取ると、ターミナルは、送信すべきデータを暗号化し、受信データの解読を開始する。したがって、基地局システムは、暗号化モード命令を送信した後に受信データの解読を開始し、また暗号化された第1のメッセージをターミナルから受信しかつ正しく復号化した後に、送信されるデータの暗号化を開始する。GSMシステムでは、暗号化モード命令は暗号化の開始命令と使用するアルゴリズムに関する情報とを含む。

【0008】

公知の方法における問題は、それらの方法が現在のシステムのために設計され、したがって、それらの方法は、1つの移動局のために複数の並列サービスが可能である新しいシステムのデータ伝送の暗号化にとって柔軟性がなく、適していないことである。同一のエアインターフェースフレームを用いて送信される2つ以上の並列プロトコルデータユニットのために同一の暗号化マスクを使用するならば、盗聴者がデータストリームから多くの情報を引き出す可能性がある。引き出すことができる情報量は、データストリームの構造に依存する。構造を持たないランダムデータから、人は情報を得ることはできないが、通常、データ内、特

に信号データ内には構造がある。

【0009】

発明の要旨

本発明の目的は、上記の問題を解決する方法、および当該方法を実施するユーザ装置および無線ネットワークサブシステムを提供することである。上記目的は、暗号化キーを生成するステップと、暗号化キーを入力パラメータとして用いて暗号化アルゴリズムに暗号化マスクを生成するステップと、暗号化マスクをプレーンデータに適用することによって、暗号化データを生成するステップとを含む、無線システムのデータ伝送を暗号化する方法において、論理チャネル特定パラメータまたは転送チャネル特定パラメータを前記暗号化アルゴリズムへの付加入力パラメータとして用いることによって達成される。

【0010】

本発明はまた、暗号化キーを生成するための生成手段と、暗号化キーを入力パラメータとして用いて暗号化マスクを生成するための生成手段と接続された暗号化アルゴリズムと、暗号化マスクをプレーンデータに適用することによって暗号化データを生成するための暗号化アルゴリズムと接続された暗号化手段と、を具備するユーザ装置に関する。暗号化アルゴリズムは、付加入力パラメータとして論理チャネル特定パラメータまたは転送チャネル特定パラメータを使用する。

【0011】

さらに、本発明は、暗号化キーを生成するための生成手段と、暗号化キーを入力パラメータとして用いて暗号化マスクを生成するための生成手段と接続された暗号化アルゴリズムと、暗号化マスクをプレーンデータに適用することによって暗号化データを生成するための暗号化アルゴリズムと接続された暗号化手段と、を具備する無線ネットワークサブシステムに関する。暗号化アルゴリズムは、付加入力パラメータとして論理チャネル特定パラメータまたは転送チャネル特定パラメータを使用する。

【0012】

本発明の好適な実施形態が、従属請求項に規定されている。

【0013】

複数の利点が本発明によって達成される。本発明の解決策において、暗号化およびその特性を柔軟に制御できる。本発明は、新しい無線システムにおけるユーザのセキュリティを強化する。この解決方法はまた、プロトコルスタックの必要とされる機能性の分散的な実施を可能にするので、エアインターフェースフレーム毎に十分に長い暗号化マスクを一度だけ使用する公知の技術よりも優れている。

【0014】

発明の詳細な説明

本発明は、種々の移動電話システムで用いることが可能である。以下の実施例では、本発明の利用は、本発明を汎用移動電話システム（UMTS）に限定することなく汎用移動電話システムについて説明する。本実施例は、UMTSのFDD（周波数分割二重）動作を示しているが、本発明をそれに限定しない。

【0015】

図1Aと図1Bを参照して、典型的な移動電話システム構成について説明する。図1Bは、本発明の説明のために本質的なブロックのみを備えるが、一般の移動電話システムが他の機能および構成も備えることが当業者には明白であり、それらについて、ここでより詳細に説明する必要はない。移動電話システムの主な部分は、コアネットワークCN、地球無線アクセスネットワークUTRANおよびユーザ装置UEである。CNとUTRANとの間のインタフェースはIuインタフェースと呼ばれ、UTRANとUEとの間のインタフェースはUuインタフェースと呼ばれる。

【0016】

UTRANは、無線ネットワークサブシステムRNSから構成される。2つのRNSの間のインタフェースはIurインタフェースと呼ばれる。RNSは、無線ネットワーク制御装置RNCと1つ以上のノードBsBから構成される。RNCとノードBとの間のインタフェースはIubインタフェースと呼ばれ、ノードBの受信領域、すなわちセルは図1AにCで示されている。

【0017】

図1Aの表示は非常に抽象的であるので、UMTSの部分に対応するGSMシ

システムの部分を記載することによって、図1Bに明瞭に示されている。UMTSの部分の使命および機能はなお計画中なので、提示したマッピングは、決して拘束的なものではなく、推量によるものであることが明らかである。

【0018】

図1Bは、移動電話システムに接続されたコンピュータ100から、インターネット102を介した、ユーザ装置UEに接続されたポータブルコンピュータ122へのパケット交換伝送を示している。ユーザ装置UEは、例えば、固定装備の無線ローカルループターミナル、車両装備のターミナルまたはハンドヘルドポータブルターミナルであり得る。

【0019】

無線ネットワークUTRANのインフラは、無線ネットワークサブシステムRNS、すなわち基地局サブシステムから構成される。無線ネットワークサブシステムRNSは、無線ネットワーク制御装置RNC、すなわち基地局制御装置と、少なくとも1つのノードB、すなわちRNC制御下の基地局とから構成される。

【0020】

ノードBは、マルチプレクサ114と、トランシーバ116と、トランシーバ116およびマルチプレクサ114の動作を制御する制御ユニット118とを備える。マルチプレクサ114は、複数のトランシーバ116によって使用されるトラフィックおよび制御チャネルを単一の伝送接続lubに配設する。

【0021】

ノードBのトランシーバ116は、二方向（あるいは時に一方向）の無線接続Uuをユーザ装置UEに提供するために使用されるアンテナユニット120との接続部を有する。無線接続Uuに伝送されるフレームの構造は詳細に決定され、また接続はエアインタフェースと呼ばれる。

【0022】

無線ネットワーク制御装置RNCは、群中継交換フィールド110と制御ユニット112とを備える。群中継交換フィールド110は、スピーチとデータとを切り替えるために、また信号回路を接続するために使用される。ノードBと無線ネットワーク制御装置RNCは基地局サブシステムを形成し、このサブシステム

は、スピーチコーデック、またはTRAU（トランスコーダ／レートアダプタユニット）108としても知られるトランスコーダをさらに備える。

【0023】

無線ネットワーク制御装置RNCとノードBの機能と物理的構造の分割は、無線ネットワークサブシステムの実際の実現に従って異なり得る。典型的に、ノードBは無線接続を実施する。無線ネットワーク制御装置RNCは、典型的に、無線資源管理、セル間ハンドオーバー制御、電力制御、タイミングと同期、およびユーザ装置用のページングを管理する。

【0024】

トランスコーダ108は、移動交換局106に可能な限り近接して通常配置されるが、この理由は、それが、トランスコーダ108とセルラ無線ネットワーク形態の無線ネットワーク制御装置RNCとの間のスピーチ伝送を可能にし、伝送容量をセーブするからである。

【0025】

トランスコーダ108は、公共交換電話網とセルラ無線ネットワークとの間で使用される異なるデジタルスピーチ符号化モードを変換して、例えば、64 k b i t / s の固定ネットワーク形態からセルラ無線ネットワークの他の形態（13 k b i t / s のような）の間に、またその逆方向で、前記公共交換電話網とセルラ無線ネットワークに互換性を与える。当然、トランスコーディングはスピーチのみのために実施される。制御ユニット112は、呼制御、移動度管理、統計データの収集およびシグナリングを実施する。

【0026】

コアネットワークCNは、UTRANの部分でない移動電話システムに属するインフラから構成される。図1Bは、コアネットワークCN、すなわち移動交換局106の部分、および外界に向かう、本実施例ではインターネット102に向かう移動電話システムインタフェースを処理するゲートウェイ移動交換局104である2つの装置を示している。

【0027】

図5は、ユーザ装置UEの模範的な構造を示している。ユーザ装置UEの本質

的な部分は、ユーザ装置UEのアンテナ502、トランシーバ506、ユーザ装置UEの制御部510とのインタフェース504、バッテリ514とのインタフェース512、およびディスプレイ500とキーボード508とマイクロホン516とスピーカ518とを具備するユーザインタフェースである。

【0028】

図2Aは、無線送信機／無線受信機対の機能を示している。無線送信機は、ノードBまたはユーザ装置に配置し得る。したがって、無線受信機は、ユーザ装置またはノードBに配置し得る。

【0029】

図2Aの上部は、無線送信機の本質的な機能性を示している。物理チャンネルに配置される異なるサービスは、例えば、スピーチ、データ、動画像または静止画像および無線送信機の制御部214で処理されるシステムの制御チャンネルである。制御部214は、装置それ自体の制御および接続の制御に関係する。図2Aは、2つの異なる転送チャンネル200A、200Bの操作を示している。異なるサービスは、異なるソース符号化装置を要求し、スピーチは例えばスピーチコーデックを必要とする。しかし、分かりやすくするため、ソース符号化装置は図2Aに示さない。

【0030】

最初に、論理チャンネルはブロック216A、216Bで暗号化される。暗号化では、暗号化されるデータは、暗号化マスクをプレーンデータに適用することによって生成される。次に、暗号化されるデータはブロック200A、200Bの転送チャンネルに配置される。後に図4A、図4C、図7Bを参考にして説明するように、暗号化は、論理チャンネルについてまたは転送チャンネルについて実行することができる。次に、異なるチャンネルは、ブロック202Aと202Bでチャンネル符号化される。チャンネル符号化の1つの形態は異なるブロックコードであり、その1つの例は巡回冗長検査、またはCRCである。チャンネル符号化を実行する他の典型的な方法は、畳込み符号化およびパンクチャド畳込み符号化とターボ符号化のようなその別形態である。

【0031】

チャネル符号化されると、チャネルはインターリーブ204A、204Bにインターリーブされる。インターリーブの目的はエラー補正をより容易にすることである。インターリーブでは、ビットは所定の方法で互いに混合され、この結果無線経路の一時的フェーディングは、必ずしも伝達情報を識別不能にしない。

【0032】

同一の送信機を用いて異なる信号を送信できるように、異なる信号がブロック208でマルチプレクスされる。

【0033】

インターリーブされた暗号化ビットは、拡散符号で拡散され、スクランブリング符号によってスクランブルされ、またブロック206で変調され、その動作は図2Bに詳述されている。

【0034】

最後に、組み合わせられた信号は、電力増幅器と帯域制限フィルタとを備え得る無線周波数部分210に搬送される。次に、アナログ無線信号がアンテナ212を介して無線経路Uuに伝送される。

【0035】

図2Aの下方部分は無線受信機の典型的な機能性を示している。無線受信機は典型的にレイク（Rake）受信機である。アナログ無線信号は、無線経路Uuからアンテナ234によって受信される。受信信号は、所望の周波数帯の外側の周波数を遮断するフィルタを備える無線周波数部分232に搬送される。次に、信号は、復調器228で中間周波数または直接ベースバンドに変換され、この形態で信号は標本化かつ量子化される。

【0036】

当該の信号はマルチパスによって伝搬された信号であるので、複数のレイクフィンガ（Rake fingers）を備えるブロック228の異なるマルチパスで伝搬された信号成分を組み合わせる努力が行われる。

【0037】

いわゆる列状のレイクフィンガでは、異なるマルチパス伝搬信号成分に関する遅延が検索される。遅延が確認された後、受信信号と、その特定のマルチパスの

確認された遅延によって遅延された使用拡散符号とを相関することによって、異なるレイクフィンガが、マルチパス伝搬信号の各々を受信するために割り当てられる。次に、復調された非拡散の異なる同一信号のマルチパスが、より強い信号を獲得するために組み合わせられる。

【0038】

次に、受信された物理チャネルは、デマルチプレクサ224で異なるチャネルのデータストリームにデマルチプレクスされる。次に、チャネルの各々はデインターリーブ226A、226Bに導かれ、ここで、受信された物理チャネルがデインターリーブされる。その後、物理チャネルは特定のチャネル復号器222A、222Bで処理され、ここで、伝送に用いられるチャネル符号化が復号化される。畳込み符号化は、ビタビ(Viterbi)復号器によって好適に復号化される。この後、転送チャネルは、ブロック200A、200Bで論理チャネルにマッピングされるか、あるいは他の可能性として、解読が転送チャネルのために実行される。チャネル復号化されたチャネル(論理または転送)は、暗号化マスクを受信データに適用することによってブロック220A、220Bで解読される。受信された各論理チャネルは、例えば、ユーザ装置UEに接続されたコンピュータ122にデータを転送することによって、さらに処理することができる。システムの制御チャネルは無線受信機の制御ユニット236に搬送される。

【0039】

図2Bは、転送チャネルが符号化され、マルチプレクスされる方法を示している。原則として、図2Bは部分的に図2Aと同じであるが、他の観点から示されている。ブロック240A、240Bでは、巡回冗長検査が各転送ブロックに加えられる。インターリーブは、ブロック242A、242B、246で2つのステージで実行される。異なる品質のサービス要求を有する2つ以上のサービスが1つ以上の物理チャネル内にマルチプレクスされる場合、サービス特定レートマッチング244が使用される。レートマッチングでは、チャネル記号レートは最適なレベルに調整され、ここで、各サービスのサービス要求の最低品質が同一のチャネル記号エネルギーによって達成される。転送チャネルの物理チャネルへのマッピングはブロック248で実行される。

【0040】

暗号化は本発明で鍵となる問題であるので、その原理について次にさらに詳細に説明する。表1では、第1の列は、受取人に伝送されなければならないプレーンデータビットを表している。第2の列のビットは暗号化マスクを構成する。暗号化マスクは、通常、排他的OR演算、すなわちXORを用いることによってプレーンデータに適用される。得られる暗号化データは第3の列にある。この暗号化データはエアインタフェースを通して受取人に送られる。次に、受取人は、送信機で用いられた同一の暗号化マスクを受信データに適用することによって、解読を実行する。第4の列は、XOR演算を用いることによって第3の列と合計される暗号化マスクである。得られた復元データは第5の列に示される。理解されるように、復元データはプレーンデータと同じである。

【表1】

プレーンデータ	0 1 1 1 0 1 0 0 1 1 1 0 0 1 1 1 0 0 0
暗号化マスク	0 0 1 0 1 0 1 0 0 0 1 0 0 0 0 1 1 1 1
暗号化データ	0 1 0 1 1 1 1 0 1 1 0 0 0 1 1 1 1 1 1
暗号化マスク	0 0 1 0 1 0 1 0 0 0 1 0 0 0 0 1 1 1 1
復元データ	0 1 1 1 0 1 0 0 1 1 1 0 0 1 1 1 0 0 0

【0041】

図3は、物理チャネルで使用されるフレーム構造の実施例を示している。フレーム340A、340B、340C、340Dには、1から72までの連続番号が与えられ、それらは720ミリ秒の長さのスーパフレームを形成する。1つのフレーム340Cの長さは10ミリ秒である。フレーム340Cは、16のスロット330A、330B、330C、330Dに分割される。スロット330Cの長さは0.625ミリ秒である。スロット330Cは、電力が例えば上方または下方に1デシベルだけ調整される1つの電力制御期間に典型的に対応する。

【0042】

物理チャネルは、共通の物理チャネルと専用物理チャネルを含む異なる型式に分割される。

【0043】

共通の物理チャネルは、PCH、BCH、RACHおよびFACHの転送チャネルを搬送するために使用される。

【0044】

専用物理チャネルは、専用物理データチャネル(DPDCH)310と専用物理制御チャネル(DPCCH)312とから構成される。DPDCH310は、OSI(開放型システム間相互接続)モデルのレイヤ2およびその上方のレイヤ、すなわち専用制御チャネル(DCH)に生成されるデータ306を搬送するために使用される。DPCCH312は、OSIモデルのレイヤ1に生成される制御情報を搬送する。制御情報は、チャネル見積もりで用いられるパイロットビット300と、フィードバック情報(FBI)308送信電力制御命令(TPC)302と、選択的に転送フォーマット結合インジケータ(TFCI)304とを含む。TFCI304は、現在のフレームで用いられている異なる転送チャネルの転送フォーマット、すなわち転送フォーマット結合について受信機に知らせる。

【0045】

図3から分かるように、ダウンリンクDPDCH310とDPCCH312は、同一のスロット330Cにタイムマルチプレクスされる。アップリンクでは、チャネルが各フレーム340CにマルチプレクスされるIQ/コード(I=同相、Q=直角位相)であるように、チャネルは並列に送られる。

【0046】

無線インタフェースUuのチャネルは、ISO(国際標準化機構)のOSI(開放型システム間相互接続)モデルに従って、3つのプロトコルレイヤ、物理レイヤ(=レイヤ1)、データリンクレイヤ(=レイヤ2)およびネットワークレイヤ(=レイヤ3)を含むプロトコルアーキテクチャに従って処理される。プロトコルスタックは、無線ネットワークサブシステムRNSおよびユーザ装置UEの両方に配置されている。各ユニット(例えば、ユーザ装置または無線ネットワ

ークサブシステム)は、他のユニットのレイヤと論理的に通信するレイヤを有する。最も低い物理レイヤのみが互いに直接連通する。他のレイヤは、常に、次の下方のレイヤについて提供されるサービスを使用する。かくして、メッセージは、レイヤの間に垂直方向に物理的に通過しなければならない、また最も低いレイヤのみでメッセージはレイヤの間を水平に通過する。図7Aはプロトコルアーキテクチャのレイヤを示している。異なるサブレイヤの間の楕円形は、サービスアクセスポイント(SAP)を示している。

【0047】

物理レイヤL1は、MACのサブレイヤMACおよび高次のレイヤに異なる転送チャンネルを提供する。如何にまたどのような特性によって、データが無線インタフェースで転送されるかについて、物理レイヤ転送サービスを説明する。転送チャンネルは、ページングチャンネルPCH、放送チャンネルBCH、同期チャンネルSCH、ランダムアクセスチャンネルRACH、順方向アクセスチャンネルFACH、ダウンリンク共用チャンネルDSCH、高速アップリンク信号チャンネルFAUSCHおよび専用チャンネルDCHを含む。物理レイヤL1は、物理チャンネルによって転送チャンネルをマッピングする。FDD(周波数分割二重)モードでは、物理チャンネルはコード、周波数によって、アップリンクでは、相対位相(I/Q)によって特徴づけられる。TDD(時分割二重)モードでは、物理チャンネルはまた、タイムスロットによって特徴づけられる。

【0048】

転送チャンネルは、共通チャンネル(特定のUEがアドレスされたときにUEのインバンド識別の必要がある場合)と、専用チャンネル(UEが、物理チャンネル、すなわちFDDとコードに関するコードと周波数、TDDに関するタイムスロットおよび周波数によって識別される場合)とに分割し得る。

【0049】

共通の転送チャンネルの型式は次の通りである。RACHは、例えば、初期アクセスまたは非リアルタイム専用制御またはトラフィックデータのかなり少量のデータを伝送するために使用される競合ベースのアップリンクチャンネルである。FACHは、かなり少量のデータを伝送するために使用される、閉ループ電力制御

なしの共通のダウンリンクチャネルである。DSCHは、専用制御またはトラフィックデータを搬送する複数のUEと共有されるダウンリンクチャネルである。BCHは、システム情報をセル全体に放送するために使用されるダウンリンクチャネルである。SCHは、TDDモードで同期情報をセル全体に放送するために使用されるダウンリンクチャネルである。PCHは、制御情報をセル全体に放送するために使用されるダウンリンクチャネルであり、効率的なUEスリープモード手順を可能にする。

【0050】

次に、専用転送チャネルの型式は次の通りである。DCHは、アップリンクまたはダウンリンクで用いられる1つのUE専用のチャネルである。FAUSCHは、FACHに関連して専用チャネルを割り当てるために使用されるアップリンクチャネルである。データリンクレイヤは、2つのサブレイヤ、すなわちMACサブレイヤ（メディアアクセス制御）およびRLCサブレイヤ（無線リンク制御）に分割される。MACサブレイヤL2/MACは、RLCサブレイヤL2/RLCに異なる論理チャネルを提供する。論理チャネルは、転送される情報の種類によって特徴づけられる。論理チャネルは、ページング制御チャネルPCCH、放送制御チャネルBCCH、同期制御チャネルSCCH、共通制御チャネル、専用制御チャネルDCCHおよび専用トラフィックチャネルDTCHを含む。

【0051】

制御チャネルは、制御プレーン情報のみの転送のために使用される。SCCHは、TDD（時分割二重）動作の場合に同期情報を放送するためのダウンリンクチャネルである。BCCHは、システム制御情報を放送するためのダウンリンクチャネルである。PCCHは、ページング情報を転送するダウンリンクチャネルである。CCCHは、ネットワークとUEとの間に制御情報を伝送するための双方向チャネルである。このチャネルは、ネットワークとのRRC接続を持たないUEによって共通に使用される。DCCHは、UEとネットワークとの間に専用制御情報を伝送する点から点の双方向チャネルである。このチャネルは、RRC接続セットアップ手順を通して確立される。

【0052】

トラフィックチャネルは、ユーザプレーンの情報のみの転送のために使用される。DTCHは、ユーザ情報の転送のための、1つのUE専用の点から点のチャネルである。DTCHは、アップリンクとダウンリンクの両方に存在できる。

【0053】

MACレイヤは、転送チャネルによって論理チャネルをマッピングする。MACサブレイヤの機能の1つは、瞬時ソースビットレートに依存する各転送チャネルのために適切な転送フォーマットを選択することである。

【0054】

図7Cは、論理チャネルと転送チャネルとの間のマッピングを示している。SCCHはSCHに接続されている。BCCHはBCHに接続されている。PCCCHがPCHに接続された。CCCHはRACHとFACHとに接続されている。DTCHは、RACHとFACHとに、RACHとDSCHとに、DCHとDSCHとに、あるいはDCHに接続できる。DCCHは、RACHとFACHとに、RACHとDSCHとに、DCHとDSCHとに、DCHに、あるいはFAUSCHに接続できる。

【0055】

第3のレイヤL3は、ユーザ装置とネットワークとの間のレイヤ3の制御プレーン信号を処理するRRCサブレイヤ（無線資源制御）を有する。RRCサブレイヤによって実施される機能には、RRC接続のための無線資源の割り当て、再構成および解放がある。したがって、RRCサブレイヤは、制御およびユーザプレーンの両方の要求を含むRRC接続に必要な無線資源の割り当てを処理する。RRCレイヤは、RRC接続の確立中に無線資源を再構築し得る。

【0056】

本発明において、我々は、一人のユーザの異なるサービスのデータフローの暗号化に関心がある。公知の技術によれば、すべてのデータフローは、同一の暗号化マスクを使用して暗号化される。

【0057】

無線システムのデータ伝送を暗号化するための本発明による方法が、図6に示されている。本方法の実行は、ブロック600において始まる。

【0058】

ブロック602では、暗号化キーは、例えば本発明の背景部分に記述されているような公知の技術に従って生成される。

【0059】

ブロック604Aでは、暗号化マスクは、暗号化キーを入力パラメータとして用いて暗号化アルゴリズムに生成される。論理チャネル特定パラメータまたは転送チャネル特定パラメータはまた、暗号化アルゴリズムへの付加入力パラメータとして用いられる。論理チャネル特定パラメータは、無線アクセスベアラ識別子、論理チャネル識別子、信号リンク識別子、または使用チャネルを識別する他のあるパラメータの1つであり得る。転送チャネルの特定のパラメータは使用された転送チャネルを識別する、例えば、専用チャネル呼識別子、あるいは何か他のパラメータであり得る。

【0060】

用語「ベアラ」は、ネットワークサービスに関連して使用される情報を伝送するための高レベルの名称である。サービスに応じて、1つ以上のベアラを用いてUMTSの情報を通常伝送することができる。例えば、サービスは、スピーチ伝送、データサービスおよびビデオサービスを含む。他方、無線ベアラは、エアインタフェースにわたって展開するベアラのその部分を表す。1つの論理チャネルは通常1つの無線ベアラを搬送する。論理チャネルは、MACレイヤによって提供されるサービスを規定する。論理チャネルは、既存のサービスモードに応じて、異なる種類の転送チャネルにマッピングすることができる（専用転送チャネルまたは共通転送チャネルに）。転送チャネルは、物理レイヤによって提供されるサービスを規定する。複数の論理チャネルをMACレイヤの1つの転送チャネルにマルチプレクスすることも可能である。さらに、転送チャネルは、物理レイヤの物理チャネルにマッピングされる。複数の転送チャネルは、レイヤ1によって1つの物理チャネルにマルチプレクスすることができる。転送チャネルのマルチプレクスの後に、データストリームを複数の物理チャネルの間に分割することが可能である。

【0061】

かくして、1つ以上の並列の無線ベアラを用いて他のトランシーバとターミナルが無線できる無線システムに、本発明を適用することができる。典型的に、呼出しがターミナルとネットワークとの間に確立されるとき、ターミナルと無線ネットワークサブシステムとの間のシグナリング無線ベアラSRBのために物理チャネルが最初に確立され、このチャネルが一旦確立されると、1つまたは複数の実際のトラフィックベアラを確立することができる。SRBは、信号リンクとも呼ぶことができる。

【0062】

伝送の方向（アップリンク／ダウンリンク）は、暗号化アルゴリズムへの付加入力パラメータとして使用することができる。

【0063】

さらにもう1つのパラメータが存在し、すなわち、暗号化アルゴリズムへの付加入力パラメータとして無線フレーム特定パラメータを使用することができる。無線フレーム特定パラメータは、例えば、ユーザ装置フレーム番号（UEFN）、または使用無線フレームを識別する他のあるパラメータであり得る。無線フレーム特定パラメータは、暗号化機能が実施されるプロトコルレイヤに依存する。暗号化機能が、UEとCNに終端するプロトコルレイヤで実施されるならば、使用フレーム番号を受信体に搬送するための機構を規定しなければならない。暗号化機能がMACレイヤまたはレイヤ1（あるいはUEとノードBまたはRNCに終端する他のあるレイヤ）に配置されるならば、少なくとも部分的に物理フレーム番号から成るフレーム番号を使用することができ、これは、使用フレーム番号をデータで信号伝送する必要がないことを意味する。

【0064】

ブロック606では、暗号化データは、例えば表1に示したようなXOR演算を用いて、暗号化マスクをプレーンデータに適用することによって生成される。

【0065】

次に、送信機および受信機における暗号化方法の実施を示した詳細な実施例について、図4A、図4B、図4Cに関連して説明する。関連する点についてのみ示すが、例えば異なった数のPDUを有する多様な状態で暗号化を実行できるこ

とが当業者には明らかであろう。

【0066】

図4Aは、本発明で規定された基本的な暗号化環境を規定するブロック図を示している。生成手段408は、公知の技術による暗号化キー410を生成するために使用される。生成手段408には、暗号化マスク412A、412B、412Cを生成するための暗号化アルゴリズム400が接続されている。暗号化アルゴリズムは、生成された暗号化キー410を入力パラメータとして使用する。暗号化アルゴリズム400は、付加入力パラメータとして論理チャネル特定パラメータ402Aを使用する。

【0067】

受信機端末では、解読のために必要な論理チャネル特定パラメータを、暗号化されていないMACヘッダから、例えばMACヘッダのC/Tフィールドから読み取ることができる。MAC PDUの構造が図8に示されている。MAC PDUは、任意のMACヘッダ800とMACサービスデータユニット(MAC SDU)802とから構成される。MACヘッダおよびMAC SDUの両方のサイズは可変である。MACヘッダ800の内容とサイズは、論理チャネルの型式に依存し、ある場合にはどのパラメータもMACヘッダ800に必要でない。MAC-SDU802のサイズは、セットアップ手順の間に規定されるRLC PDUのサイズに依存する。MACヘッダ800はC/Tフィールド804を備える。この選択は、異なる論理チャネル(または同一の論理チャネル型式の異なるインスタンス)を1つの転送チャネルに、専用転送チャネルと共通転送チャネルの両方に、効率的にMACマルチプレクスするのを可能にする。この方法を使用する場合、MACヘッダは暗号化されず、これによって、受信機端末の異なるMAC PDUの分離が可能になり、また共通チャネルモードでは、UTRANの正しい実体にメッセージをルーチンするために必要なRNTI(無線ネットワーク一時識別子)フィールドの読取りが可能になる。

【0068】

暗号化アルゴリズム400には、暗号化マスク412A、412B、412Cをプレーンデータ414A、414B、414Cに適用することによって、暗号

化データ418A、418B、418Cを生成するための暗号化手段416A、416B、416Cが接続されている。図4Aから分かるように、プレーンデータは、少なくとも2つの並列論理チャネルからの無線リンク制御レイヤプロトコルデータユニットを含み、また各論理チャネルのために個々の暗号化マスクが生成される。したがって、図4Aでは、したがって、暗号化マスク412A、412Bおよび412Cはすべて互いに異なる。

【0069】

ブロック420では、暗号化されたRLC-PDUは、MACレイヤを通して処理され、1つの転送ブロックセット、すなわちMAC PDUセットにマッピングされる。

【0070】

他の可能な解決策は、プレーンデータが、1つのみの論理チャネルからの1つの無線リンク制御レイヤプロトコルデータユニット414Aを含む解決策であり、また前記論理チャネルのために個々の暗号化マスク412Aが生成される。したがって、本発明はまた個々の論理チャネルのためにも機能する。

【0071】

通常、プロトコルスタックの物理レイヤの各無線フレームのために、新しい暗号化マスクが生成される。インターリーブが使用されるならば、プロトコルスタックの物理レイヤの各インターリーブ期間について新しい暗号化マスクを生成することができる。典型的に、1つのインターリーブ期間は複数の無線フレームから構成される。

【0072】

図4Aの左側は、送信機で実施される動作を示している。図4Aの右側に示されているように、対応する動作は受信機においても実施される。唯一の差は、受信された転送ブロックセットからRLC-PDUを導くためにブロック422が使用されることであり、また受信データを解読するために解読手段424A、424B、424Cが使用されることである。

【0073】

本発明の1つの実施形態では、少なくとも1つ論理チャネルの無線リンク制御

レイヤプロトコルデータユニットは、すでに暗号化されており、また暗号化データを生成するステップは、前記すでに暗号化された無線リンク制御レイヤプロトコルデータユニットのために繰り返されない。かくして、データを2度暗号化することが避けられる。当然、例えばこのような端末から端末への暗号化が使用されるならば、データを2度、すなわち最初にサービスを用いた適用によって、次に本発明によるMACレイヤによって暗号化することができる。これによって、たとえ暗号化が2度実行されとしても、XOR演算は余分のビットを加えないので、送信容量の損失は引き起こされない。

【0074】

図4Bは、プレーンデータが、1つの論理チャネルの少なくとも2つの連続した無線リンク制御レイヤプロトコルデータユニットを含む状態に対する解決策を示している。例えば、第1のRLC PDU 414Aおよび第2のRLC PDU 414Bが1つの論理チャネルからであると仮定するならば、問題は、これらのPDU 414A、414Bのために1つのみの暗号化マスク 412Aを生成するような方法で解決することができる。次に、この暗号化マスク 412Aの異なる部分は、第1のPDU 414Aと第2のPDU 414Bとを暗号化するために使用される。この場合に必要な暗号化マスク 412Aの長さは、当然、第1および第2のPDU 414A、414Bの長さの和である。PDU 414A、414Bは同一の論理チャネル（同一の無線アクセスベアラ）からなので、必要とされる最大長は、そのベアラの最大RLC PDUサイズの2倍であると計算され得る。

【0075】

図4Cは、プレーンデータが、少なくとも2つの異なる論理チャネルのメディアアクセス制御レイヤプロトコルデータユニットを含む1つの転送ブロックセット(TBS)を有する状態を示し、各転送ブロックセットのために、暗号化データを生成する際に1つの暗号化マスク 412が使用される。この選択では、暗号化される基本単位は転送ブロックセットである。これは、アルゴリズム400によって製造される暗号化マスク 412の必要な長さを規定する。レイヤ1は、転送ブロック特定のCRC（巡回冗長検査）をなお加えるが、XOR演算はデータ

の長さを変えないので、TBS全体を1つの単位として暗号化できなければならない。TBSの各転送ブロックの長さは、いずれにせよL1に伝えなければならない。この選択は、MACヘッダもまた暗号化され、したがって、TBSを解読する前に、MAC PDUをネットワーク側のどこにも導くことができないという不都合を有する。これは、L1上の共通チャネルが可能であるならば、問題である。必要な暗号化マスク412の長さは、当該の転送チャネルのための最大転送ブロックセットサイズに等しい。

【0076】

他の可能な解決策は、プレーンデータが、1つの論理チャネルのメディアアクセス制御レイヤプロトコルデータユニットを含む解決策であり、各転送ブロックセットのために、暗号化データを生成する際に1つの暗号化マスク412が使用される。

【0077】

本発明の解決策は、好ましくはソフトウェアによって無線システムで実施され、この場合、本発明は、送信機および受信機に、特に図2Aのブロック204A、204Bおよび226A、226Bに配置されるプロトコル処理ソフトウェアに、ある機能を必要とする。かくして、生成手段408、暗号化アルゴリズム400および暗号化手段416A、416B、416Cは、ユーザ装置UEおよび無線ネットワークサブシステムRNSに存在するプロトコルスタックのソフトウェアモジュールであり得る。解決策はまた、例えばASIC（特定用途向け集積回路）または別個のコンポーネントを用いてハードウェアによって実施することができる。

【0078】

本発明の方法は、例えば、プロトコルスタックのメディアアクセス制御レイヤで実施することができる。これは図7Bに示され、本図は、含まれる暗号化機能について図7Aに示されたMACレイヤの高レベルの概要を示している。C1（）およびC2（）は、暗号化の位置の2つの選択肢である。C1（0）、C1（1）、C1（2）およびC1（3）は、図4Aと図4Bを参考にして上に説明したような論理チャネル特定暗号化パラメータの使用を示し、これに対し、C2（

00)、C2(01)およびC2(02)は転送チャネル特定暗号化パラメータの使用を示している。あるMAC機能がC2(00)、C2(01)およびC2(02)ブロックの下で必要とされるかもしれないが、分かりやすさのため、それらはここでは図示しない。基本的に、RLC PDUは各論理チャネルからMACレイヤに来る。MACレイヤでは、次に、RLC-PDUは、PCH、BCH、SCH、専用チャネル用の動作および共通チャネル動作を含む機能ブロック700、702、704においてMAC PDUにマッピングされる。通常、1つのRLC PDUは1つのMAC PDU(=転送ブロック)にマッピングされる。このマッピングによって、論理チャネルから転送チャネルへのマッピングが実現される。マッピング規則は図7Cに関連して上に説明してある。暗号化がCCCHのために使用されるならば、暗号化ブロック、例えばC1(4)は、図7Bで「CCCH」と機能ブロック704との間のラインの中になければならない。

【0079】

本発明について、添付図面に示した実施例を参考にして上に記述してきたが、本発明がその実施例に限定されず、添付請求項に開示した創意に富んだ構想内の多くの方法で変更し得ることが明白である。

【図面の簡単な説明】

【図1A】

移動電話システムの例(その1)である。

【図1B】

移動電話システムの例(その2)である。

【図2A】

送信機と受信機を示している。

【図2B】

転送チャネルの符号化および多重化を示している。

【図3】

フレーム構造を示している。

【図4A】

本発明による暗号化環境のブロック図（その 1）である。

【図 4 B】

本発明による暗号化環境のブロック図（その 2）である。

【図 4 C】

本発明による暗号化環境のブロック図（その 3）である。

【図 5】

移動局を示している。

【図 6】

本発明による方法を示したフローチャートである。

【図 7 A】

プロトコルスタックの例を示している。

【図 7 B】

本発明によるプロトコルスタックの例を示している。

【図 7 C】

論理チャネルと転送チャネルとの間のマッピングを示している。

【図 8】

メディアアクセス制御レイヤプロトコルデータユニットの構造を示している。

【図1A】

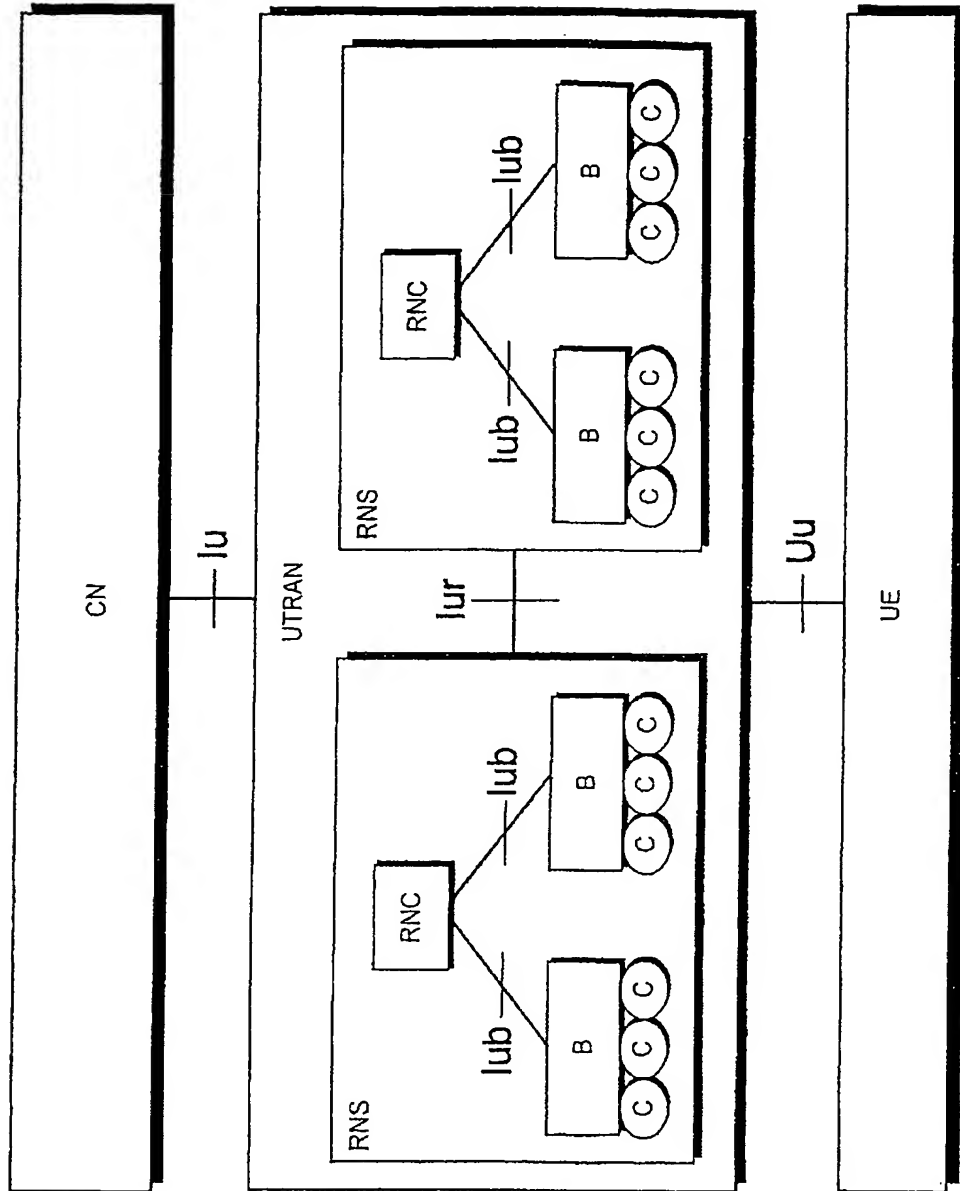


Fig 1A

【図1B】

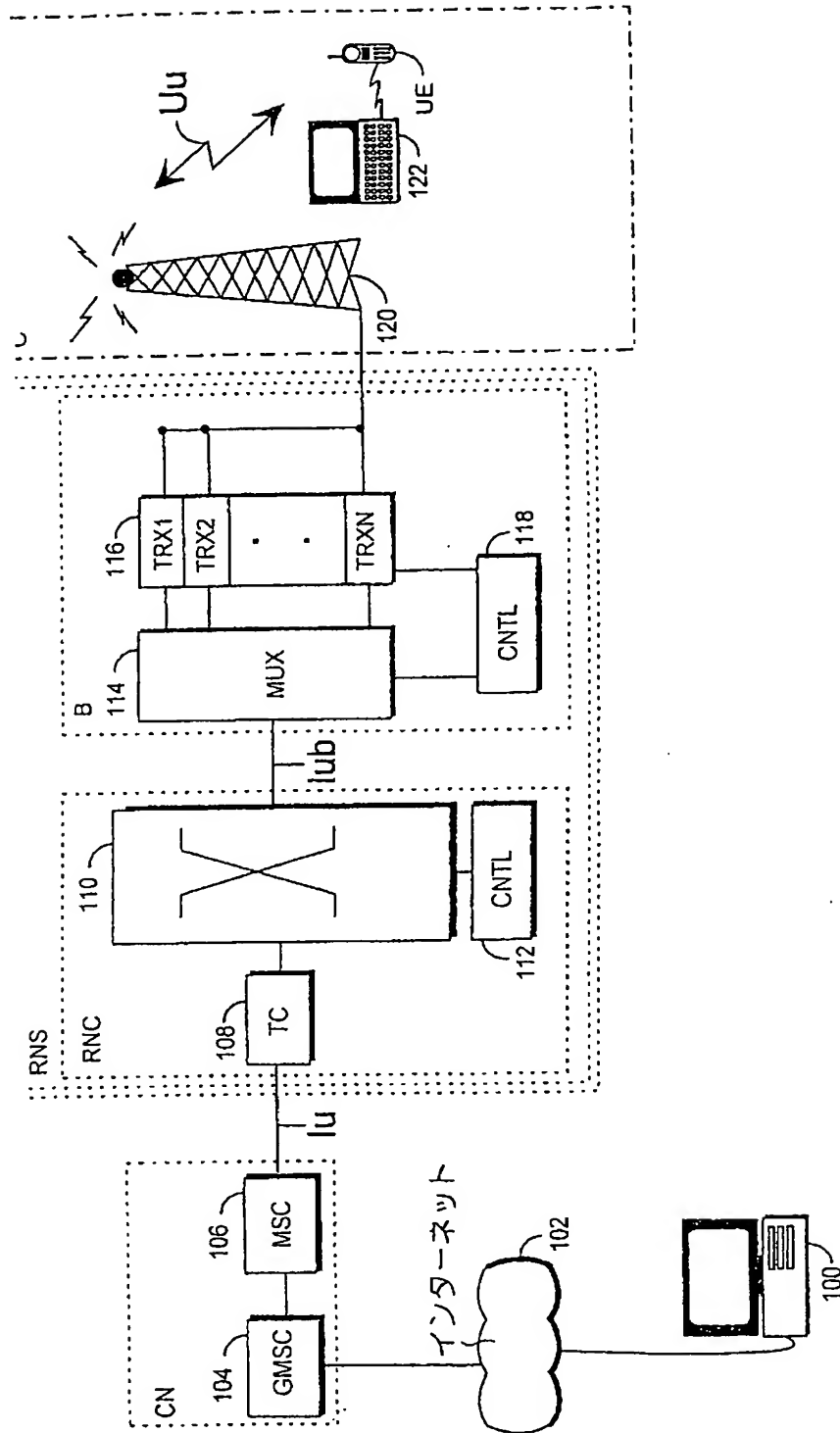


Fig 1B

【図 2 A】

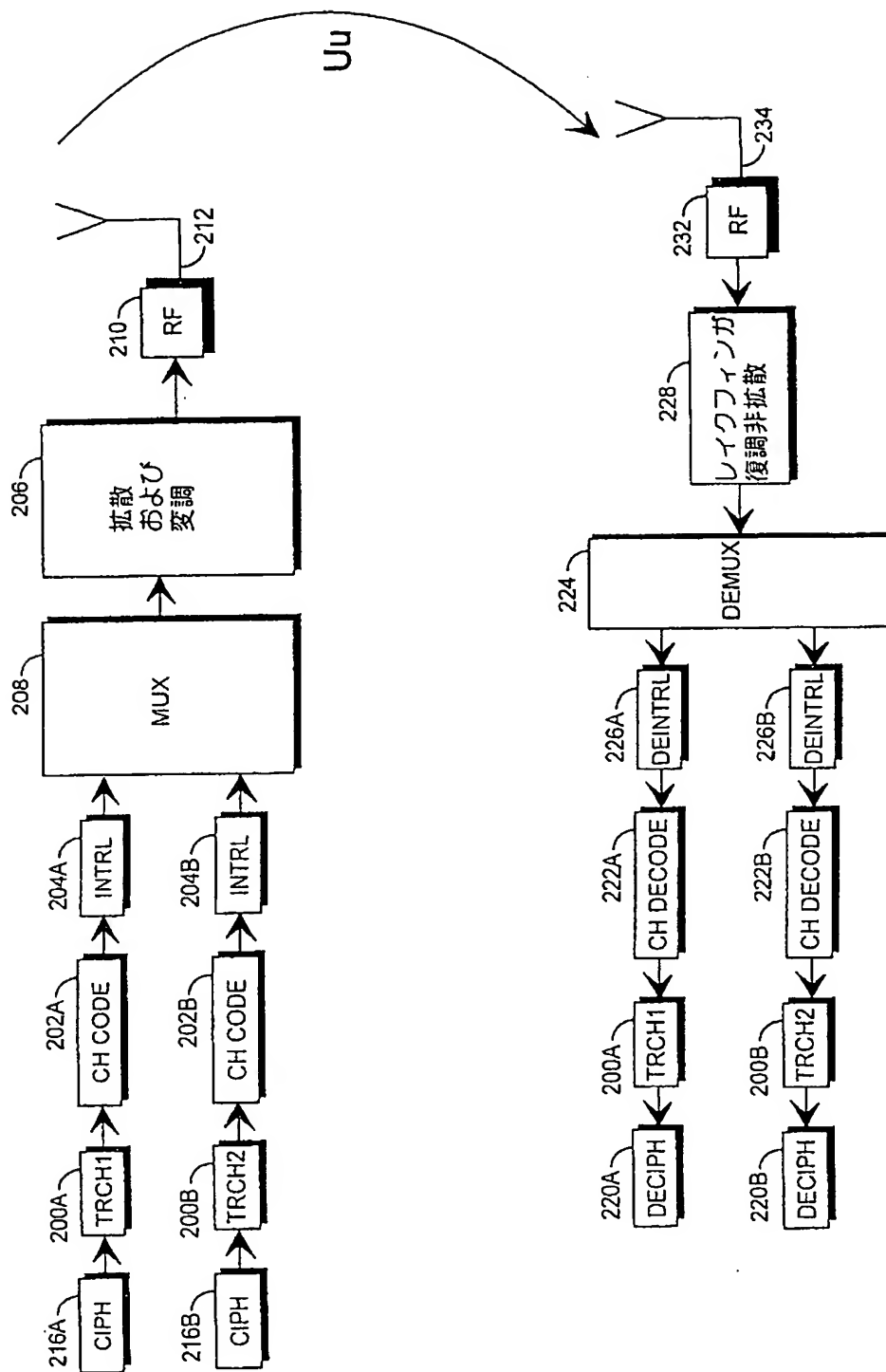


Fig 2A

【図 2 B】

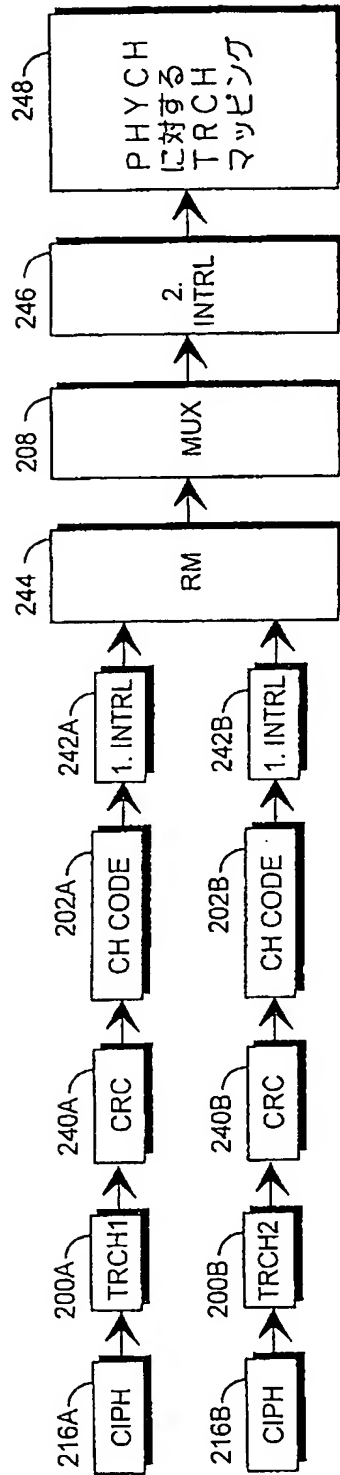


Fig 2B

【図4A】

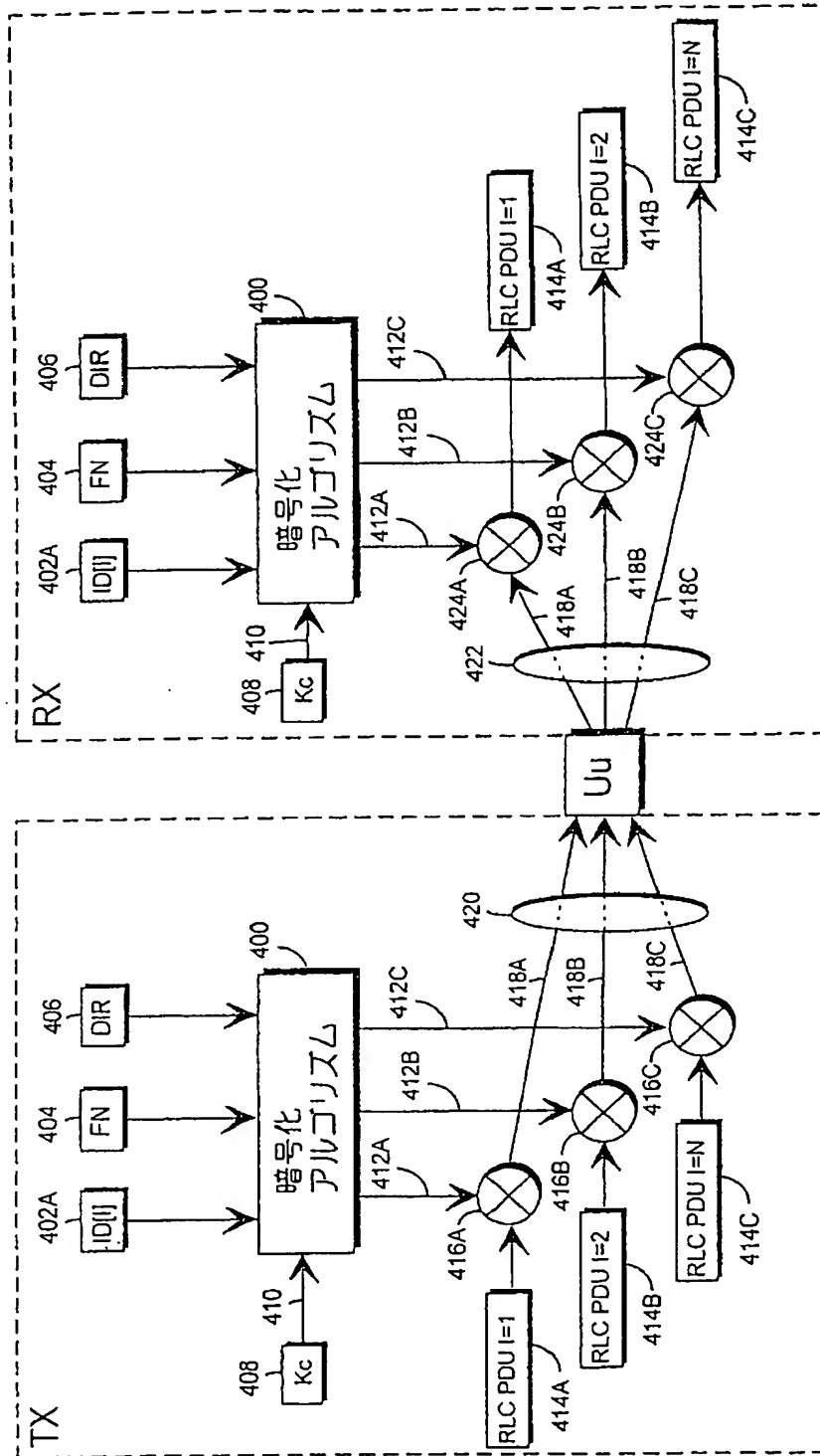


Fig 4A

【図 4 B】

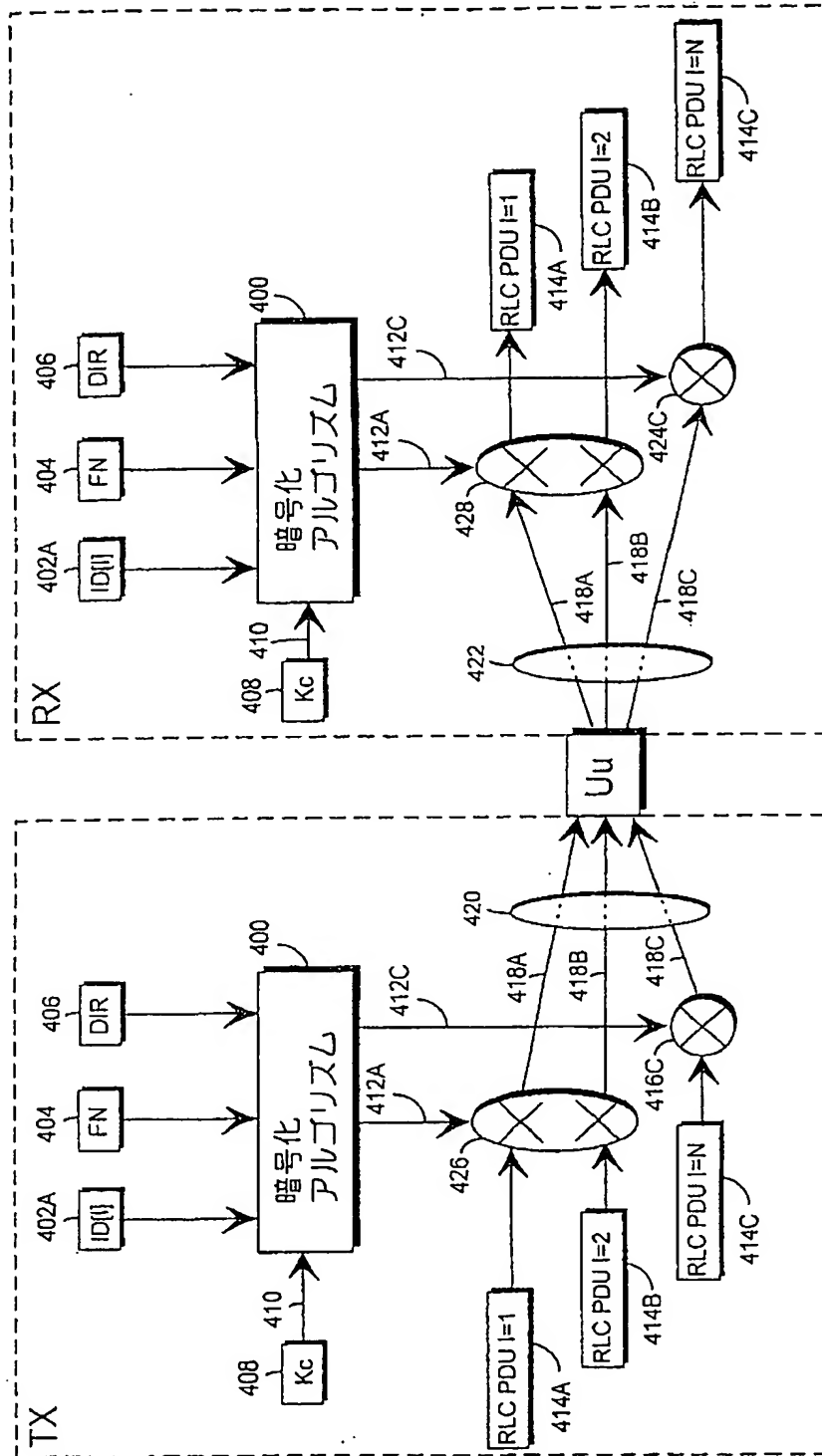


Fig 4B

【図 4C】

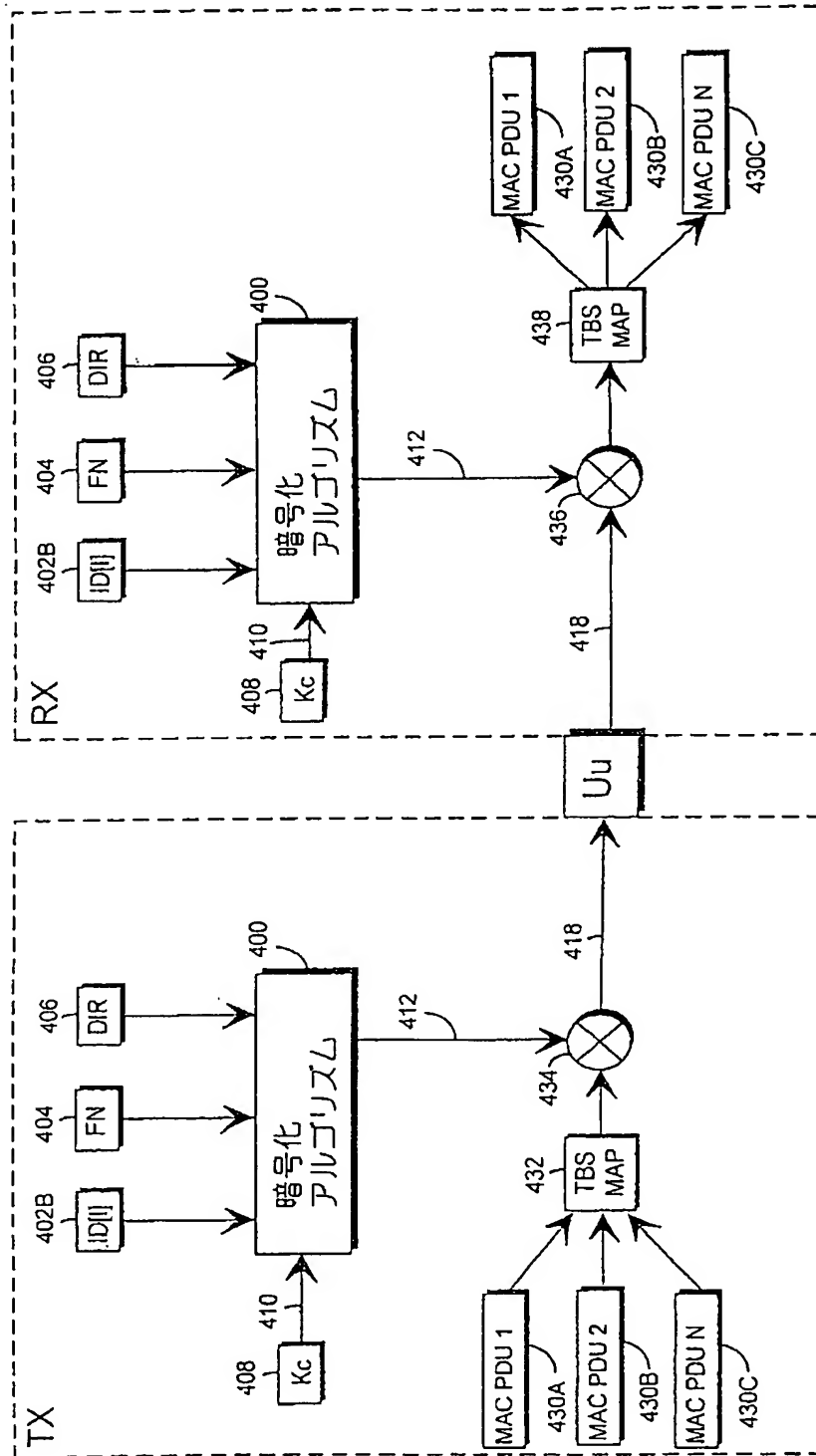


Fig 4C

【図5】

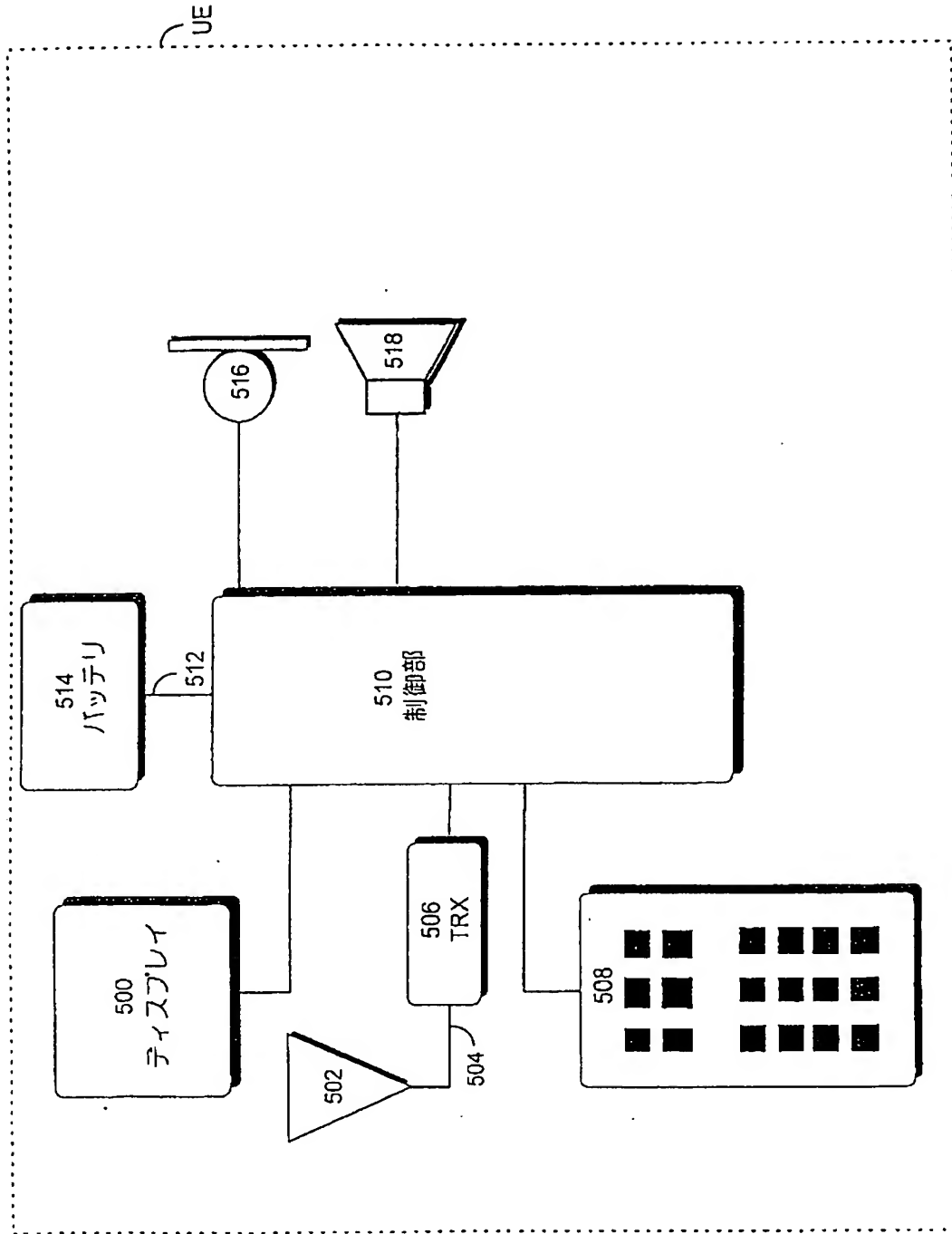


Fig 5

【図6】

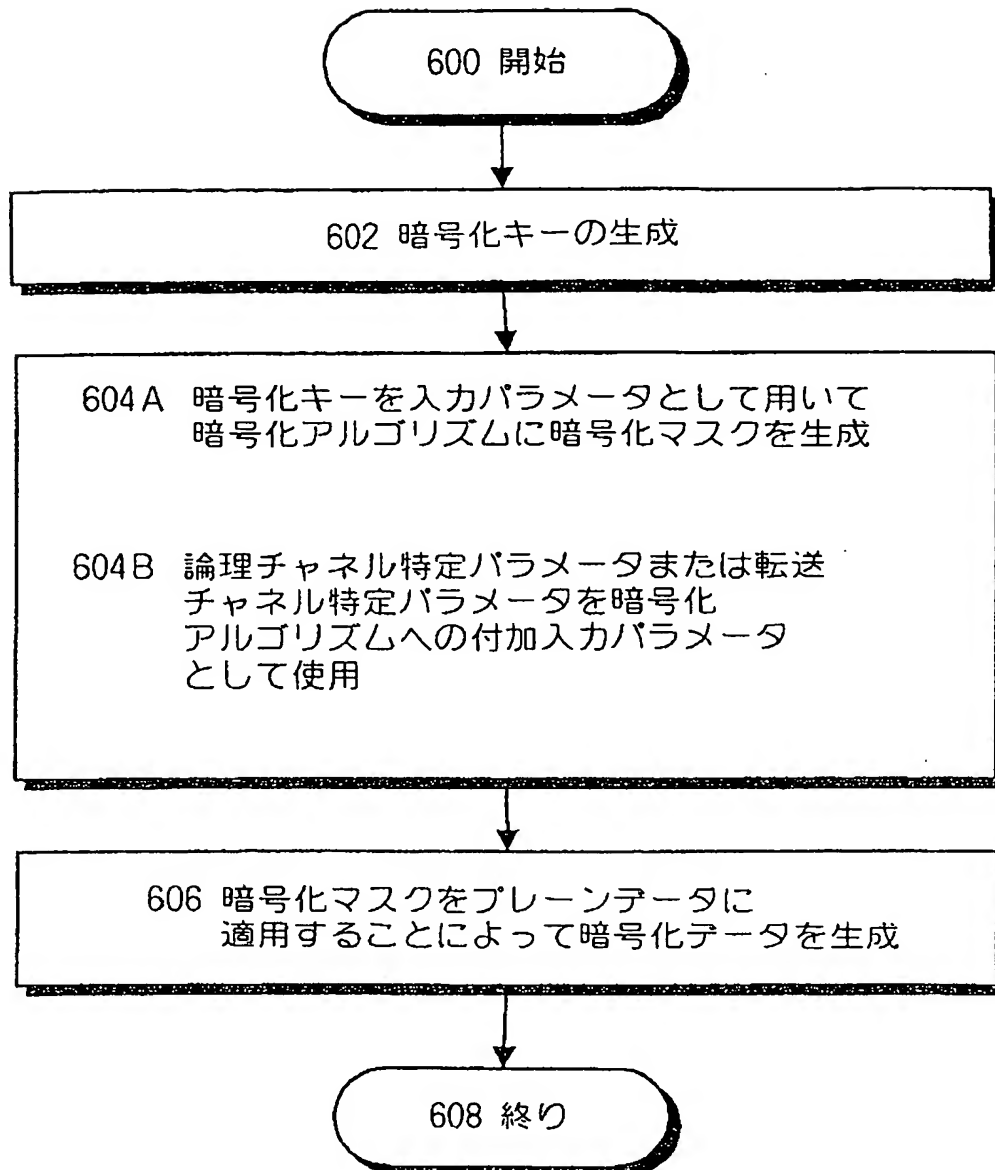


Fig 6

【図7A】

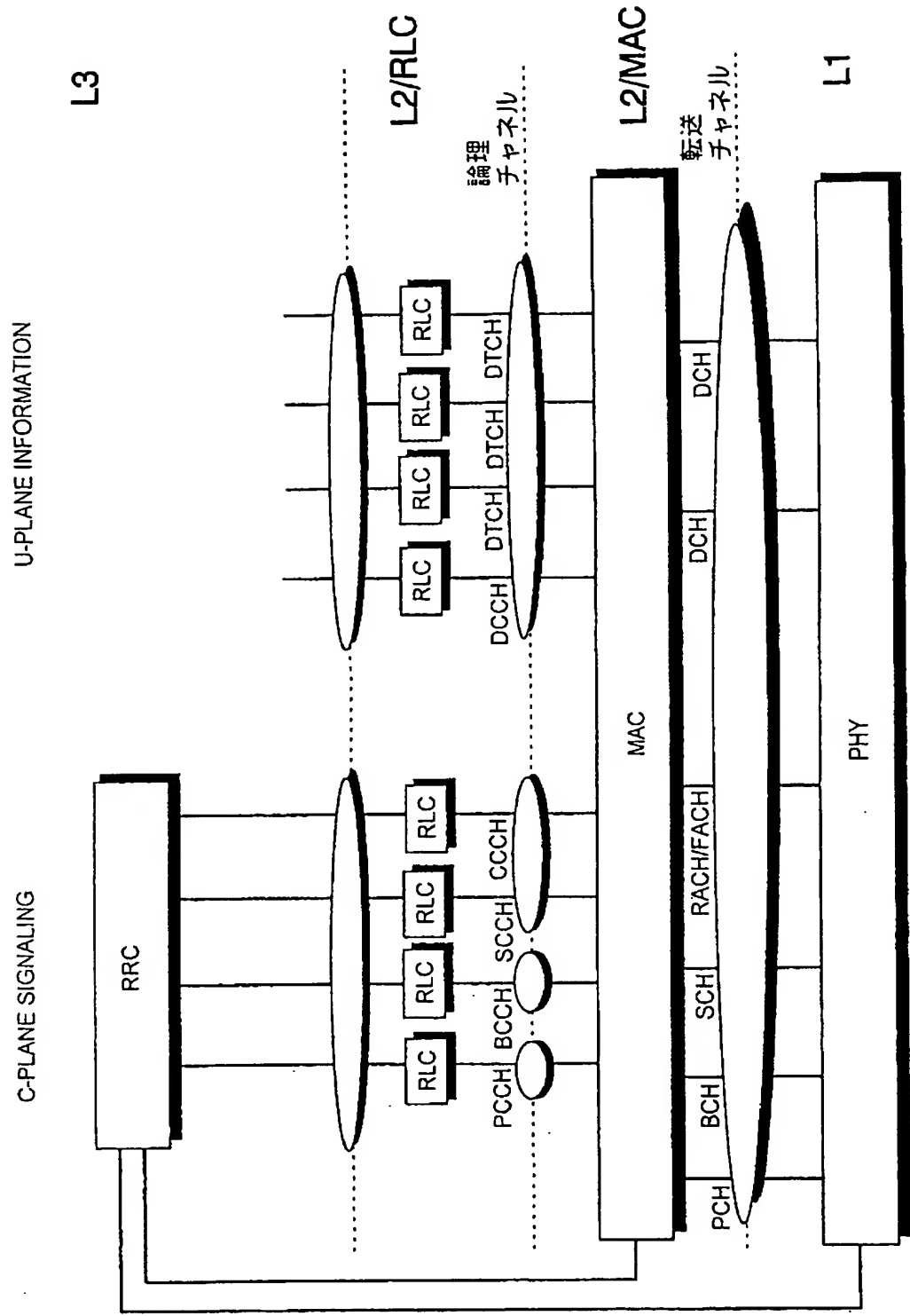


Fig 7A

【図 7 B】

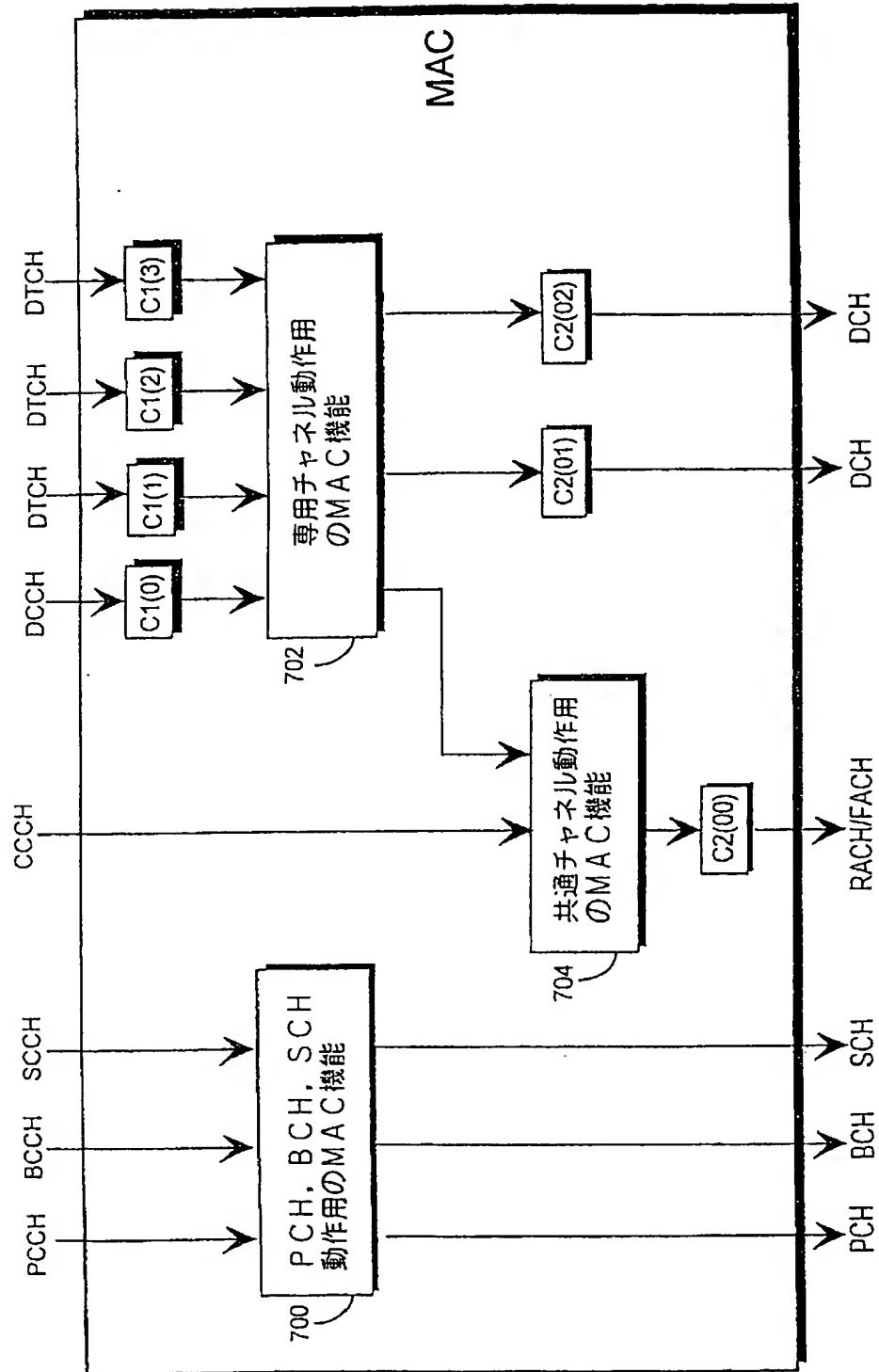


Fig 7B

【図 7 C】

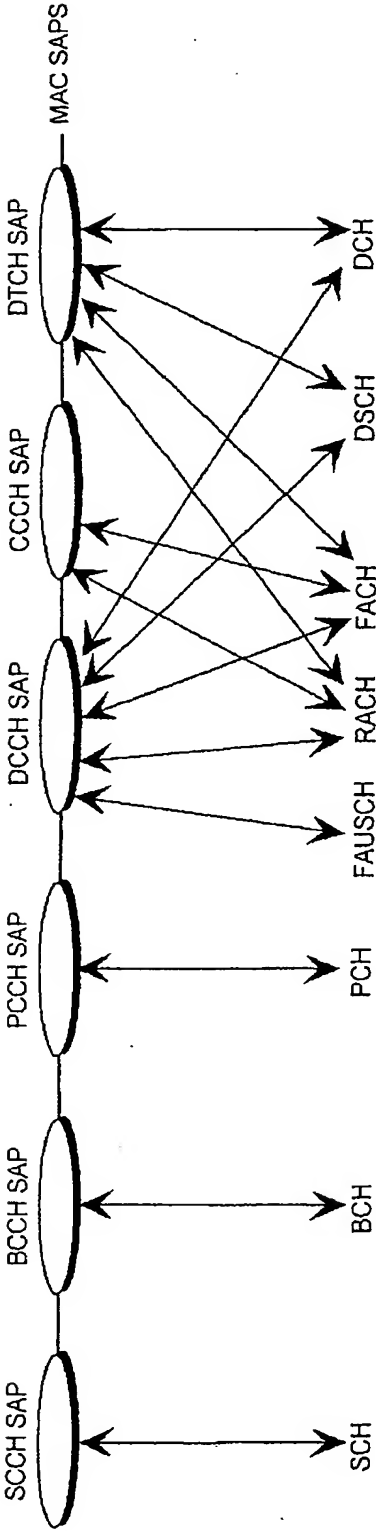


Fig 7C

【図 8】

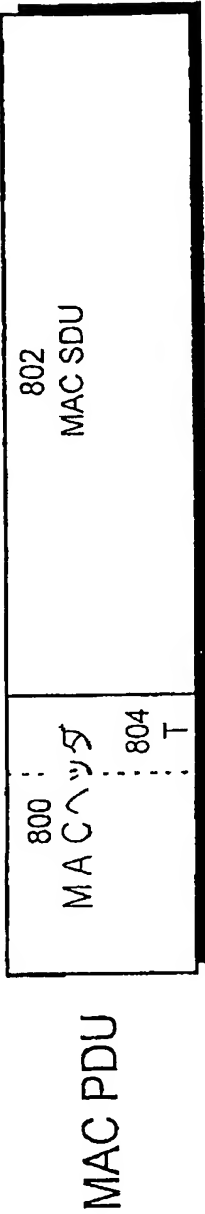


Fig 8

【国際調査報告】

1

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI 00/00177

A. CLASSIFICATION OF SUBJECT MATTER		
IPC7: H04L 9/16 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
IPC7: H04L		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
SE,DK,FI,N0 classes as above		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9712461 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)), 3 April 1997 (03.04.97), claim 1	1,16,31
A	--	2-15,17-30, 32-45
A	US 5600722 A (T. YAMAGUCHI ET AL.), 4 February 1997 (04.02.97), see the whole document	1-45
	-- -----	
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
3 August 2000		04 -08- 2000
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86		Authorized officer Rune Bengtsson/AE Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT
 Information on patent family members

02/12/99

International application No.

PCT/FI 00/00177

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9712461 A1	03/04/97	AU 7102196 A	17/04/97
		CA 2233463 A	03/04/97
		CN 1198278 A	04/11/98
		EP 0872078 A	21/10/98
		JP 11511629 T	05/10/99
		NZ 318911 A	29/06/99
		SE 506619 C	19/01/98
US 5600722 A	04/02/97	SE 9503343 A	28/03/97
		JP 7107083 A	21/04/95
		US 5604807 A	18/02/97

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW

Fターム(参考) 5J104 AA32 BA04 NA02

5K067 AA30 BB04 BB21 DD17 EE02

EE10 FF02 HH22 HH24 HH36

KK15